Well Known Port Usage in IP communications Mandated

1. PURPOSE

This addendum addresses the IONet Security Policy standard port specifications to reduce the risk to the IONet from non-standard IP networking connections. The use of non-standard ports for networking traffic is a practice that has not been previously addressed in the IONet Security Policy.

2. SCOPE

The scope of this addendum includes non-standard port communications traversing the IONet, including the Open, Restricted, and Closed IONet zones.

3. APPLICABILITY

This addendum applies to all zones of the IONet: Open, Closed, and Restricted, and applies to all systems connecting to these IONet zones. It is applicable to all NASA field centers, stations, facilities, NASA program offices, NASA contractors, international partner agencies, universities, and commercial ground stations with IONet access or interface(s).

This addendum is immediately applicable to new system connections and new implementations of standard port communications. Existing non-standard port implementations will be transitioned into alignment with this policy within one (1) years of this addendum. This policy is valid for up to 3 years from the signatures date, or until superseded.

4. AUTHORITY, APPLICABLE POLICY, and GUIDANCE

The IONet Network Security Officer (NSO) has the authority to develop, implement, and manage policies, processes, and procedures to protect the confidentiality, integrity, and availability of the IONet. The NSO also has the authority to ensure that connected systems are operating in such a manner that ensures the safety of other connected systems and the IONet itself. The NSO shall ensure that NASA's policy and requirements are developed consistent with applicable statutory authority, including:

a. Federal Information Security Management Act (FISMA) and the associated Special Publications from National Institute of Standards and Technology (NIST).

b. Federal Information Processing Standards (FIPS) publications (PUB) promulgated by NIST.

c. NASA Procedures and Requirements (NPR) 2810.1-A Security of Information Technology

5. DEFINITIONS

For the purposes of this policy the following definitions apply.

Well Known Ports	The port commonly used for a particular standard IP service or protocol. For example http traffic is generally run on port 80. For instance, TCP Ports 0-1023.
Non-standard port	Any port that is not commonly and generally used for well known IP services. For example transporting FTP traffic on port 5000.
Internet Protocol (IP)	IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source

6. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This policy was not addressed in the IONet Security Policy, 700-DOC-029.

7. POLICY

All systems connecting to the IONet shall adhere to the requirements specified herein. Any IONet-connected device found to be in violation of this policy will be disconnected from the IONet and/or permission to enter the area will be rescinded. The device will be blocked from the IONet until it is brought into compliance and has passed an IONet vulnerability scan.

7.1 Requirements

The following requirement must be met by devices connected to the IONet.

IONet-connected hosts must adhere to the port number assignments as defined by IANA (http://www.iana.org/assignments/port-numbers) for IP network services.

Matthew Kirichok
IONet Network Security Officer

Bradford Torain

Bradford Torain
IONet System Owner